UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE ACCOUNTS d.alba.phd2020@gmail.com; st.hill.optic20@gmail.com; AND sa.ha.2109sa@gmail.com THAT IS STORED AT PREMISES CONTROLLED BY GOOGLE LLC	Case No. 24-mj-86-01-TSM **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Christine Chambers, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with certain accounts that is stored at premises controlled by Google LLC (hereinafter, "Google" or "PROVIDER"), an email and web services provider headquartered in Mountain View, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

2. I am a Special Agent of the United States Department of Commerce, Bureau of Industry and Security ("BIS"), Office of Export Enforcement ("OEE"), currently assigned to the Boston Field Office located in Marlborough, Massachusetts, and have been so employed since August 2018. Prior to being employed with OEE, I was employed as a Special Agent with the

U.S. Army Criminal Investigations Division – Major Procurement Fraud Unit beginning in July 2014. Prior to that, beginning in 2010, I was a Special Agent for the 902d Military Intelligence Group where I conducted Counterintelligence Investigations. I have received specialized training on how to conduct investigations involving the illegal export of sensitive technology, weapons, and other controlled commodities, and on the federal criminal statutes that regulate and, in certain instances, prohibit the export of controlled commodities, including weapons, weapons systems, and military equipment and technology. I have participated in several investigations of violations of United States laws relating to the unlawful export from the United States of commodities, software, and technology restricted for export. I am familiar with many investigative techniques employed to investigate such offenses, including search warrants for the search of email accounts, computers, digital media, and associated media storage.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents, witnesses, and agencies. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only; all sums or amounts are approximate and are not full and final amounts; and all dates and times are on or about those indicated.

4. The Federal Bureau of Investigation ("FBI") and OEE are currently investigating David ALBA, Stiven HILL and Suzhang LEE[1] for export control violations and related offenses.

[1] As discussed further below, it is presently unknown whether ALBA, HILL, and LEE are the true identities of actual persons. All references to these individuals are intended to describe a person acting under that identity, whether real or fictitious.

Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of the Export Control Reform Act of 2018 (ECRA), 50 U.S.C. §§ 4801 *et seq.*; 13 U.S.C. § 305 (failing to file or filing false electronic export information); and 18 U.S.C. § 371 (conspiracy) have been committed by ALBA, HILL, and LEE, and other known and unknown participants in the above-referenced scheme.

5. There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

LEGAL BACKGROUND

Export Control Reform Act and Export Administration Regulations

7. The Export Administration Regulations ("EAR") control, among other things, the export and re-export to foreign countries of dual-use items, a term that encompasses commercial items that also have a military application. The EAR place limitations on the export of those goods and technologies that the Secretary of Commerce deems could make a significant contribution to the military potential of other countries, could prove detrimental to the national security of the United States, or are contrary to the foreign policy of the United States. EAR controls are based not only on the nature of the item but also on its destination, end-use, and end-user.

8. Among other things, section 734.3 of the EAR provides (subject to limited exceptions) that all items in the United States, and all U.S.-origin items wherever located, are "subject to the EAR." 15 U.S.C. § 734.3(a)–(b). An export is an actual shipment or transmission of items subject to the EAR out of the United States. 15 C.F.R. § 734.13(a)(1). The EAR generally prohibit any person from exporting or causing the export from the United States of a controlled commodity without having first obtained a validated export license from the U.S. Department of Commerce, unless an exception applies. The Commerce Department maintains the Commerce Control List ("CCL"), which specifies the goods and technologies that require export licenses.

9. The most sensitive items subject to EAR controls are identified on the CCL. 15 C.F.R. part 774, Supp. No. 1. Items on the CCL are categorized by Export Control Classification Number ("ECCN") based on their technical characteristics. Each ECCN has export control requirements (including licensing requirements) depending on destination, end user, and end use. Separately, the "EAR99" designation is used for items subject to other general provisions of the EAR, but not listed with a specific ECCN on the CCL.

10. ECRA provides that "it shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of this subchapter or of any regulation, order, license or other authorization issued under this subchapter," 50 U.S.C. § 4819(a)(1), including the following specific unlawful acts enumerated in 50 U.S.C. § 4819(a)(2):

> (A) No person may engage in any conduct prohibited by or contrary to, or refrain from engaging in any conduct required by this subchapter, the Export Administration Regulations, or any order, license or authorization issued thereunder.
>
> (B) No person may cause or aid, abet, counsel, command, induce, procure, permit, or approve the doing of any act prohibited, or the omission of any act required by this subchapter, the Export Administration Regulations, or any order, license or authorization issued thereunder.

***

(E) No person may order, buy, remove, conceal, store, use, sell, loan, dispose of, transfer, transport, finance, forward, or otherwise service, in whole or in part, or conduct negotiations to facilitate such activities for, any item exported or to be exported from the United States, or that is otherwise subject to the Export Administration Regulations, with knowledge that a violation of this subchapter, the Export Administration Regulations, or any order, license or authorization issued thereunder, has occurred, is about to occur, or is intended to occur in connection with the item unless valid authorization is obtained therefor.

***

(G) No person may engage in any transaction or take any other action with intent to evade the provisions of this subchapter, the Export Administration Regulations, or any order, license, or authorization issued thereunder.

***

11. Under 50 U.S.C. § 4819(b), it is unlawful for a person to willfully commit, attempt to commit, conspire to commit, or aid and abet in the commission of an unlawful act described in 50 U.S.C. § 4819(a).

Export Documentation Violations

12. For all exports valued over $2500, or for which an export license is required for shipment outside of the United States, the U.S. seller, manufacturer, exporter, or its shipping agent is required to file detailed information with the United States government, which enables the government "to prevent the export of certain items to unauthorized destinations and/or end users." 15 C.F.R. § 30.1(b). This information is submitted electronically by filing EEI in the Automated Export System ("AES"). EEI includes, among other things, detailed information about the seller, manufacturer, or exporter; the date of export; the ultimate end-user; the country of ultimate destination; the value of the goods being exported; the ECCN; and if applicable, the export license number. By filing this information with the United States government, the filer is certifying that the EEI information is true, accurate, and complete. 15 C.F.R. § 758.1(f).

Knowingly providing false or misleading information, or causing such information to be provided, in connection with the preparation and submission of "export control documents," including EEI filings, is a violation of the EAR. 15 C.F.R. § 764.2(g)(1)(ii); *see also* 15 C.F.R. § 772.1 (defining an "Export control document" to include, among other things, "Electronic Export Information (EEI) on the Automated Export System (AES) presented in connection with shipments to any country"). Similarly, concealing information from the Department of Commerce or U.S. Customs Service by failing to file EEI in connection with an export also violates the EAR. 15 C.F.R. § 764.2(g)(1).

13. Under 13 U.S.C. § 305, "[a]ny person who knowingly fails to file or knowingly submits false or misleading export information through the Shippers Export Declaration (SED) (or any successor document) or [the AES] shall be subject to a fine not to exceed $10,000 per violation or imprisonment for not more than 5 years, or both."

PROBABLE CAUSE

14. Thorlabs, Inc., is a company located in Newton, New Jersey that designs and manufactures products in the areas of fiber optics, lasers, optical instrumentation, opto-mechanics, photonics and vibration isolation. From June 15 to August 9, 2023, Thorlabs received approximately 6 orders from an individual who identified himself as David ALBA. ALBA purported himself to be affiliated with the University of New Hampshire. The orders were for a variety of relatively low value, EAR99 items, such as a motorized polarization controller, PM fiber isolator, fixed optical attenuator and patch cables. For these orders, ALBA listed his "bill to" address as University of New Hampshire, 23 College Road, Parsons Hall, Durham, NH. ALBA listed the "ship to" address as 10 Delaware Dr., Suite 1, Box 1054416, Salem, NH.

15. For one such order, on June 15, 2023 a Thorlabs Customer Service Representative communicated with David ALBA via email at d.alba.phd2020@gmail.com concerning an order recently placed by ALBA.

16. The Representative told ALBA he had answered "YES" for export and requested the name of the company/university and the country the items were to be exported to. ALBA provided the following response: "The option to export outside of America was not selected correctly and a mistake occurred on my part, and I emphasize that I do not intend to export outside of America."

17. On or about November 28, 2023, Thorlabs received a web order application from Stiven HILL, who also identified himself as a being affiliated with the University of New Hampshire. The order was for one ULN15TK Turnkey Ultra-Low-Noise Laser System, 1550nm, 12mW, PM Fiber, FC/APC. The total cost of the order was $13,040. The Billing and Shipping information was provided to Thorlabs as Stiven Hill, University of New Hampshire, 10 Delaware Dr., Suite 1, Box 1054416, Salem, NH 03079. Email: st.hill.optic20@gmail.com.

18. Thorlabs lists the ULN15TK Turnkey Ultra-Low-Noise Laser System as being ECCN 6a995.n.1. As part of its routine export compliance procedures, Thorlabs requires customers to fill out an End User/End Use statement for all items with an ECCN other than EAR99. HILL provided Thorlabs an End User Statement indicating HILL was the End User, and the End Use stated "For use in research projects as Optical Reference Laser." HILL signed and dated this statement on Nov 28, 2023.

19. On December 6, 2023, Thorlabs received a SWIFT payment for $13,040 from "ARMANIS ENDUSTRIYEL MAKINE TEKS.T." The wire transfer detail report indicates that these funds originated in Istanbul, Turkey.

20. On December 12, 2023, a Thorlabs customer service representative entered into an online chat initiated by HILL regarding the laser system order. During the chat, the representative questioned HILL's affiliation with University of New Hampshire and asked HILL if the order was intended to be exported to Iran. Below is the verbatim chat exchange:

info [Automated], 12 Dec. 2023, 8:14am

Thank you for choosing to chat with us. An agent will be with you shortly.

info [Automated], 12 Dec. 2023, 8:14am

You are now chatting with Jackie.

Jackie, 12 Dec. 2023, 8:14am

Hello

Jackie, 12 Dec. 2023, 8:14am

How can I help you.

Stiven, 12 Dec. 2023, 8:14am

Hello,

Did you receive the payment for Quotation TQ0520439?

I have also sent you the receipt and payment

Jackie, 12 Dec. 2023, 8:15am

Let me check

Jackie, 12 Dec. 2023, 8:16am

We have not received payment. Please email a copy of the bank receipt to AR@thorlabs.com

Jackie, 12 Dec. 2023, 8:17am

This is for the University of New Hampshire ?

Stiven, 12 Dec. 2023, 8:18am

yes

Jackie, 12 Dec. 2023, 8:18am

Is this being exported to Iran?

Stiven, 12 Dec. 2023, 8:19am

No, I didn't understand what you meant

Jackie, 12 Dec. 2023, 8:21am

Is this going to be shipped to Iran. Your visitor's information on chat states Iran

Stiven, 12 Dec. 2023, 8:22am

I think there is a mistake, I don't understand what you mean

Jackie, 12 Dec. 2023, 8:23am

That is fine.

Jackie, 12 Dec. 2023, 8:23am

Is there anything else I can help you with.

Stiven, 12 Dec. 2023, 8:24am

I added a new order to my card, will I get a discount?

Stiven, 12 Dec. 2023, 8:24am

NUW1411383

Stiven, 12 Dec. 2023, 8:25am

؟؟؟

Jackie, 12 Dec. 2023, 8:26am

A discount will be provided if the order qualifys for one.

Stiven, 12 Dec. 2023, 8:27am

Where can the discount amount be seen?

Jackie, 12 Dec. 2023, 8:28am

We will send you a PDF file of the order. The discount if applicable would be stated.

IP INFORMATION INDICATING HILL WAS COMMUNICATING FROM IRAN

21. The "Visit Info" associated with the above chat indicated HILL was communicating via a desktop device from Tehran, Iran with Internet Protocol ("IP") address 5.250.52.234.

22. The Internet Corporation for Assigned Names and Numbers ("ICANN") is an internationally organized, non-profit corporation that has responsibility for IP address space allocation, protocol identifier assignment, and other server management functions. ICANN allocates IP address blocks to the five Regional Internet Registries (RIR) around the world, who in turn, allocate smaller IP address blocks to service providers and ultimately to the user. The American Registry for Internet Numbers ("ARIN") is one of the prominent RIRs. ARIN offers public access to Internet resource registration data via a number of services. These services are known in the industry as "Whois."

23. On April 2, 2024, an open source Whois query of this data for the IP address 5.250.52.234 indicated the IP address was located in Iran.

INFORMATION FROM UNH AND BOXIT4ME

24. The University of New Hampshire confirmed, via the Deputy UNH Police Chief, that, neither David ALBA nor Stiven HILL have any past nor present association with the University. UNH also confirmed it is not associated with the ship to address of 10 Delaware Dr. Box 1054416, Salem, NH.

25. 10 Delaware Dr., Suite 1, Salem, NH is the location of a company called Boxit4me, a consolidation and repackaging company. Investigators went to that location and spoke with the site manager, who stated that the majority of shipments received at Boxit4me are consolidated, repackaged, and exported to various freight forwarders located abroad, including in Dubai, United Arab Emirates.

26. Boxit4me, through corporate counsel, provided the following account holder information for Box 1054416.

Mr. Suzhang LEE

China Passport: E96050424

DOB: April 15, 1997

Email: sa.ha.2109sa@gmail.com

27. Boxit4me provided agents with a copy of the passport used to open the account. Agents noted the name on the passport did not match the name coded on the bottom of the passport, indicating the passport was likely fraudulent.

28. Boxit4me provided the shipping history for Box 1054416. The information showed the Boxit4me account was registered on July 12, 2021. From February – December 2023, Box 1054416 received 22 shipments, all of which were consolidated and exported to Dubai, UAE over eight shipments during the same time period.

29. There is evidence that at least one such shipment contained products from Thorlabs and had a final destination of Iran. The Thorlabs order dated June 26, 2023, reference number NUW1379669, and sales order number TS3321747-1, was delivered to 10 Delaware St, Box 1054416, Salem, NH on June 27, 2023.

30. Boxit4me records included a spreadsheet containing tracking information for Box 1054416. Specifically, shipment number 6 included the following information:

Order Start Date: 7/18/2023

Order Delivery Date: 7/26/2023

Complete Delivery Address: Um rammul. Marakesh St. 17 st Dubai comer city. Warehouse section. Number A02, Dubai, United Arab Emirates

Shipper and tracking information: SkyExpress; AWB 5101688292

Incoming shipment tracking number NUW137669

31. A query of the above-referenced AWB tracking number 5101688292 on the SkyExpress website indicated the following:

Reference No. 64374

Consignee Name: c/o Syed Shoaib Hider +971-568679914

Destination: Dubai

Status: Delivered

Delivery Date and Time: 26 Jul, 2023 16:15

Receiver Name: Marie May

Shipment Type: Non-Documents

32. A public Instagram page for a company called Dubai to Iran Express provides the phone number +971-568679914 (matching the consignee name for the SkyExpress shipment containing the Thorlabs products shipped from Boxit4me to Dubai). Dubai to Iran Express markets itself as a transhipper from the UAE to Iran, offering "Direct Delivery from Dubai to Tehran in the fastest time!"

33. Thus, it appears that ALBA, HILL, LEE, and others presently unidentified, have obtained products from Thorlabs for end use in Iran, using a series of shipments (from Thorlabs to Boxit4me to Dubai to Tehran) in violation of the export control laws of the United States.

34. Accordingly, I have probable cause to believe that ALBA, HILL, and LEE have engaged, and are engaging, in an illegal scheme including the unlawful export of items on the CCL to Dubai and Iran. I further have probable cause to believe that ALBA, HILL, and LEE have provided false descriptions and valuations for goods being shipped in order to evade EEI

filing requirements, and have failed to file EEI as required for certain exports to Iran. In addition, I have probable cause to believe that a search of the SUBJECT ACCOUNTS will reveal evidence of the same.

35. Preservation letters were sent to the PROVIDER in December 2023 and February 2024 for the following email accounts.

- d.alba.phd2020@gmail.com
- st.hill.optic20@gmail.com
- sa.ha.2109sa@gmail.com

BACKGROUND CONCERNING EMAIL

36. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail ("email") access, to the public. Google allows subscribers to obtain email accounts at the domain name "@gmail.com," such as the email accounts listed in Attachment A. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google's services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

37. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience,

evidence of who was using an email account may be found in address books, contact lists, email in the account, and attachments to emails, including pictures and files.

38. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

39. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

40. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mailbox" on Google's servers until the subscriber deletes the email. If the subscriber does not

delete the message, the message can remain on Google's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

41. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

42. Information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account, along with the time and date of that access. By

determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

43. Based on the forgoing, I request that the Court issue the proposed search warrant.

44. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on PROVIDER. Because the warrant will be served on PROVIDER, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

45. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because

their premature disclosure may give targets an opportunity to flee from prosecution, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

Respectfully submitted,

/s/ Christine Chambers
Christine Chambers
Special Agent
U.S. Department of Commerce, Bureau of Industry and Security, Office of Export Enforcement

The affiant appeared before me by telephonic conference on this date pursuant to Fed. R. Crim. P. 4.1 and affirmed under oath the content of this affidavit and application.

Date: **Apr 25, 2024**

Hon. Talesha Saint-Marc
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with d.alba.phd2020@gmail.com; st.hill.optic20@gmail.com; and sa.ha.2109sa@gmail.com; that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at Mountain View, California.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the "Provider")

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A:

a. The contents of all emails associated with the account from July 2021 to Present, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. All records or other information stored by an individual using the account, including address books, contact lists, calendar data, pictures, and files; and

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government within 14 days of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence, fruits, and instrumentalities of violations of the Export Control Reform Act of 2018 (ECRA), 50 U.S.C. §§ 4801 *et seq.*; 13 U.S.C. § 305 (failing to file or filing false electronic export information); and 18 U.S.C. § 371 (conspiracy), those violations involving David ALBA, Stiven HILL and Suzhang LEE and others presently unknown occurring after July 1, 2021, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

(a) Information that constitutes evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with the Account about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts;

(b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(c) Evidence indicating the email account owner's state of mind as it relates to the crimes under investigation;

(d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(e) The identity of the person(s) who communicated with the user ID, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, law enforcement agents may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by Google LLC ("Google"), and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of Google. The attached records consist of _____. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of Google, and they were made by Google as a regular practice; and

b. such records were generated by Google's electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of Google in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by Google, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

Date	Signature